


| | | |
|--|---------------------------------------|-------------------------------------|
|  <p style="text-align: center;">MILITARY HEALTH SYSTEM (MHS)</p> <p style="text-align: center;">INFORMATION ASSURANCE (IA)</p> <p style="text-align: center;">IMPLEMENTATION GUIDE</p> | IMPLEMENTATION GUIDE No. 8 | |
| | EFFECTIVE DATE 07/19/05 | REVISED DATE xx/xx/xx |
| Subject: <p style="text-align: center;">CERTIFICATION AND ACCREDITATION (C&A)</p> | | |

1 PURPOSE AND SCOPE

The provisions of this guide are policy for all TRICARE Management Activity (TMA) Components (TRICARE Management Activity (TMA) Directorates; TRICARE Regional Offices (TRO), and the Program Executive Office (PEO), Joint Medical Information Systems Office (JMISO)) (hereafter referred to as the TMA Component(s)). For TRICARE Contractors, this document is policy if required by contract; otherwise it serves as information assurance guidance. The Chief Information Officers of the Service Medical Departments are encouraged to incorporate this document into their information assurance policies and procedures.

MHS Certification and Accreditation (C&A) is a four-phase process consisting of definition, verification, validation, and post accreditation that applies to all the TMA Component and contractor ISs, including networks. The MHS C&A process is conducted in accordance with current DoD C&A guidance. The primary purpose of the MHS C&A process is to protect and secure the elements that make up the MHS information infrastructure, regardless of where the IS is located. The MHS C&A procedures shall be utilized in conjunction with current DoD C&A guidance and DoDI 8500.2, "Information Assurance (IA) Implementation," dated February 6, 2003. All DoD ISs shall be reaccredited within three years of the effective date of the system's Approval to Operate (ATO) or when significant changes occur to impact the security posture of the systems. The MHS C&A process must be monitored and maintained throughout the system's development life cycle. Key information technology (IT) personnel shall adhere to the MHS C&A process for any government-owned or contractor-owned IS that transmits, processes, stores, or accesses DoD unclassified information, DoD sensitive information, and/or connects to any DoD system or network during acquisition, operation, and throughout the system life cycle.

2 POLICY

- 2.1 The MHS shall conduct C&A for all MHS ISs (government-owned or contractor-owned) that transmit, process, store, or access DoD sensitive information and/or connect to any DoD system or network. The MHS IA Program also requires TRICARE contractors to comply with C&A requirements. The MHS shall utilize current DoD C&A guidance as its

baseline to maintain a sound IA posture throughout the MHS IS infrastructure. Throughout all the phases of MHS ISs development, information owners must include and utilize the guiding principles of current DoD C&A guidance.

- 2.2 The MHS IA Program Office shall ensure that all planning activities are scheduled and maintained to ensure MHS ISs that require C&A are managed effectively. The registration and management of ports, protocols, and services shall also be addressed as part of the C&A process. Upon recommendation from their respective Certification Authorities (CAs), the Designated Approving Authorities (DAAs) shall authorize, via letter to the MHS IS Program Managers (PM), an Interim Approval To Operate (IATO) for a maximum period of one year (if required), or an Approval To Operate (ATO) for a maximum period of three years. A Certification Authority/Certifier shall be designated by the DAA with the authority to establish and manage the organization's C&A program and to verify and validate IS security design and implementation through testing and review of IS security documentation. An annual review will be performed as a part of the C&A process to review contingency plans, changes in to DoD Ports, Protocols, and Services Management, and security controls. Approximately seven months prior to the expiration of the system's accreditation, or when significant changes occur or are projected to occur, the System Owner must request reaccreditation or an IATO. An IATO is reserved for ISs that have not been certified or accredited, and yet for operational reasons, must be deployed before completing certification or accreditation, or for accredited systems that cannot complete their recertification before their current certification expires.

3 RESPONSIBILITIES

- 3.1 The Director, MHS IA Program shall:
 - a. Ensure TMA and TRICARE contractor ISs are accredited and undergo reaccreditation every three years, or sooner in the event that significant changes occur to impact the security posture of the system.
 - b. Contact the PM or System Owner when the IS is scheduled for an annual review or recertification.
 - c. Provide assistance and guidance, when necessary, to programs and projects that are preparing for, undergoing, and complying with current DoD C&A requirements.
- 3.2 Service Medical Chief Information Officers shall:
 - a. Ensure their respective Service-specific ISs and contractor ISs are certified and accredited and undergo reaccreditation every three years, or sooner in the event that significant changes occur to impact the security posture of the system.
 - b. Contact the PM or contractor Point of Contact (POC) prior to when the IS is scheduled for an annual review or recertification.
 - c. Provide assistance and guidance, when necessary, to programs and projects that are preparing for, undergoing, and complying with current DoD C&A requirements.

3.3 The JMISO PEO shall:

- a. Ensure TMA Centrally Managed ISs are certified and accredited and undergo re-accreditation every three years, or sooner in the event that significant changes occur to impact the security posture of the system.
- b. Contact the PM or contractor POC prior to when the IS is scheduled for an annual review or recertification.
- c. Provide timely coordination, assistance, and guidance, when necessary, to programs and projects that are preparing for, undergoing, and complying with current DoD C&A requirements.

3.4 The DAA shall:

- a. Ensure that Information Assurance Managers (IAMs), Information Assurance Officers (IAOs), and System Administrators (SAs) are established in writing and are designated for all systems under their jurisdiction, and that they receive the level of training and certification necessary to perform the tasks associated with their assigned responsibilities.
- b. Ensure the reaccreditation of ISs and networks at least every three years, or whenever previously accredited systems undergo major modifications.
- c. Approve or deny IATOs in a timely manner so as not to delay operational requirements.
- d. Verify that an appropriate mission assurance category has been assigned for each IS/network under his/her jurisdiction.

3.5 PMs shall:

- a. Provide resources to perform C&A of systems, applications, and networks under their control throughout the life cycle.
- b. Utilize guidance specified in MHS C&A standard operating procedures and detailed instructions in references (a), through (d) in section 6.
- c. Ensure C&A is accomplished prior to deployment of newly developed ISs and/or networks.
- d. Ensure risk assessment is performed as part of C&A.
- e. Request an IATO as soon as the security evaluation determines the need.
- f. Maintain ISs' security controls to comply with current DoD IA policies and directives.
- g. Identify security deficiencies and take action to achieve an acceptable security level.
- h. Verify data ownership, accountability, and access rights, and ensure all special handling requirements are established for each IS/network under his/her jurisdiction.
- i. Ensure that all Health Insurance Portability and Accountability Act (HIPAA) Security requirements are met in accordance with reference (g) for all ISs/networks that process, store, transmit, or access protected health information (PHI).
- j. Ensure processes for reporting security incidents and lessons learned are established.

- k. Ensure that security safeguards approved during accreditation are implemented and maintained as necessary throughout the system life cycle.
 - l. Ensure that an IA awareness, training, and education program is implemented for all users, to include developers, SAs, operators, and managers.
 - m. Document Memorandums of Agreement (MOAs) and Memorandums of Understanding (MOUs) to address security requirements between ISs that interface or are networked and managed by different DAAs.
 - n. Document MOAs and MOUs to address security requirements between ISs that are interfaced or networked to non-DoD entities. If these connections process PHI, then appropriate Business Associate Agreements addressing HIPAA Security requirements must also be in place.
 - o. Software (operation system or applications) additions, changes, or upgrades providing security features (e.g., additional functional and capability modules).
- 3.6 The Certification Authority/Certifier shall:
- a. Establish and manage C&A program.
 - b. Ensure verification and validation IS security design and implementation through testing and review the of IS security documentation.
 - c. Review contingency plans and security controls on annual basis, or when significant changes occur.
 - d. Prepare C&A report with system certification recommendations for the DAA.

An annual review will be performed as a part of the C&A process to review contingency plans and security controls. Approximately seven months prior to the expiration of the system's accreditation, or when significant changes occur or are projected to occur, the System Owner must request reaccreditation or an IATO. An IATO is reserved for ISs that have not been certified or accredited, and yet for operational reasons, must be deployed before completing certification or accreditation, or for accredited systems that cannot complete their recertification before their current certification expires.

4 IA SECURITY REQUIREMENTS

- 4.1 IA Security requirements shall be established for all MHS ISs. Security requirements shall consist of, but are not limited to, administrative, personnel, physical, environmental, and technical controls which shield the IS against sabotage, tampering, denial of service, espionage, fraud, misappropriation, misuse, modification, destruction, and data disclosure. The security requirements shall be satisfied through a combination of administrative, automated, and manual means in a cost-effective and integrated fashion. All TMA Component and contractor ISs shall be evaluated to ensure minimum security standards are implemented and enforced in accordance with references (a) through (f) in section 6.

5 REACCREDITATION

- 5.1 In accordance with current DoD C&A procedures, ISs shall be reaccredited every three years, or sooner if a significant change to hardware, software, or environment occurs. The following is a list of events affecting security that may require ISs to be recertified and reaccredited:
- a. Level of criticality and/or sensitivity change for the system/environment impacting reliable baseline countermeasures.
 - b. Hardware additions, changes, or upgrades requiring a change in the approved security countermeasures.
 - c. Software (operating system or applications) additions, changes, or upgrades (e.g., additional functional and capability modules).
 - d. Security policy (e.g., access control policy) changes.
 - e. Threat change creating system vulnerability resulting in a higher risk.
 - f. Mission changes requiring a different security mode of operation.
 - g. Breaches of security, system integrity, or unusual situations that appear to invalidate the accreditation by revealing flaws in security design exposing its vulnerability.
 - h. Significant changes in the physical structure of the facility or the system is moved to a different facility.
 - i. Significant changes in operating procedures.
 - j. System configuration changes (e.g., a workstation connected outside of the approved accreditation parameters).
 - k. Networks - Inclusion of additional (separately accredited) system(s) affecting the security of that system.
 - l. Networks - Modification/replacement of a subscribing system affecting the security of that system.
 - m. Results of an audit or external analysis.
 - n. Addition of system interfaces with other systems.

6 REFERENCES

- a. DoDI 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," December 30, 1997
- b. DoD 8510.1-M, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual," July 31, 2000
- c. DoDD 8500.1, "Information Assurance (IA)," October 24, 2002
- d. DoDI 8500.2, "Information Assurance (IA) Implementation," February 6, 2003
- e. Federal Information Security Management Act of 2002

- f. Public Law 104-191, “Health Insurance Portability and Accountability Act of 1996,” August 21, 1996
- g. CNSSI No. 4009, “National Information Assurance (IA) Glossary,” May 2003

7 ACRONYMS

| | |
|---------------|---|
| ATO | Approval to Operate |
| C&A..... | Certification and Accreditation |
| CA..... | Certification Authority |
| DAA..... | Designated Approving Authority |
| DITSCAP | DoD Information Technology Security Certification and Accreditation Process |
| DoD..... | Department of Defense |
| DoDD..... | Department of Defense Directive |
| DoDI | Department of Defense Instruction |
| HIPAA | Health Insurance Portability and Accountability Act |
| IA | Information Assurance |
| IAM..... | Information Assurance Manager |
| IAO | Information Assurance Officer |
| IATO..... | Interim Approval to Operate |
| IS | Information System |
| IT..... | Information Technology |
| JMISO..... | Joint Medical Information Systems Office |
| MHS..... | Military Health System |
| MOA | Memorandum of Agreement |
| MOU | Memorandum of Understanding |
| PEO | Program Executive Officer |
| PHI | Protected Health Information |
| PM..... | Program Manager |
| POC..... | Point of Contact |
| SA | System Administrator |
| TMA..... | TRICARE Management Activity |
| TRO..... | TRICARE Regional Offices |